

A NOTE ON THE MOMENTS OF KLOOSTERMAN SUMS

PING XI AND YUAN YI

ABSTRACT. In this note, we deduce an asymptotic formula for even power moments of Kloosterman sums based on the important work of N. M. Katz on Kloosterman sheaves. In a similar manner, we can also obtain an upper bound for odd power moments. Moreover, we shall give an asymptotic formula for odd power moments of absolute Kloosterman sums. Consequently, we find that there are infinitely many $a \bmod p$ such that $S(a, 1; p) \gtrsim 0$ as $p \rightarrow +\infty$.

1. INTRODUCTION

Let p be an odd prime. For any integer a and b , the classical Kloosterman sum is defined by

$$S(a, b; p) = \sum_{x \bmod p}^* e\left(\frac{ax + b\bar{x}}{p}\right),$$

where the summation is over a reduced residue system mod p . Such an exponential sum first appeared in a paper of H. Poincaré [Po] on modular functions. As tackling the problem on the representation of numbers in positive definite diagonal quadratic forms, H. D. Kloosterman [Kl] re-introduced and first seriously studied the exponential sum $S(a, b; p)$, which was later named after him. He proved for any odd prime p that

$$(1) \quad |S(a, b; p)| \leq 3^{1/4} p^{3/4}, \quad (ab, p) = 1.$$

The best result up to now is due to A. Weil [We]

$$(2) \quad |S(a, b; p)| \leq 2p^{1/2}, \quad (ab, p) = 1,$$

the proof of which originally requires deep results of algebraic geometry. At present, due to the important work of S. A. Stepanov, W. Schmidt and E. Bombieri, Weil's bound can be established by elementary means. See [Sch] for details.

Kloosterman sums play quite an important role in modern analytic number theory, as well as the theory of automorphic forms (see [Iw] for instance). One of the problems is to consider the moments of Kloosterman sums, namely

$$V_k(p) = \sum_{a \bmod p}^* S^k(a, 1; p).$$

The original motivation to consider the moments just follows H. D. Kloosterman, who wished to gain a nontrivial bound for the individual sum. This leads him to consider the problem in a global sense first. For the cases $k \leq 4$, we can give exact identities by elementary methods. To be precise, we have

$$\begin{aligned} V_1(p) &= 1, \\ V_2(p) &= p^2 - p - 1, \\ V_3(p) &= \left(\frac{p}{3}\right)p^2 + 2p + 1, \end{aligned}$$

2010 *Mathematics Subject Classification.* 11L05.

Key words and phrases. Kloosterman sum, mean value.

$$V_4(p) = 2p^3 - 3p^2 - 3p - 1,$$

where $(\frac{\cdot}{p})$ is the Legendre symbol mod p . The last one was first obtained by H. D. Kloosterman, which enables him to deduce the first nontrivial bound (1).

For the case of $k = 5$, it follows from the work in [Li, PTV] that

$$V_5(p) = \left(\frac{p}{3}\right)4p^3 + (a_p + 5)p^2 + 4p + 1, \quad p > 5,$$

where a_p is the integer with $|a_p| < 2p$ defined for $p > 5$ by

$$a_p = \begin{cases} 2p - 12u^2, & \text{if } p = 3u^2 + 5v^2, \\ 4x^2 - 2p, & \text{if } p = x^2 + 15y^2, \\ 0, & \text{if } p \equiv 7, 11, 13 \text{ or } 14 \pmod{15}. \end{cases}$$

For $k = 6$, H. Salié [Sa] and H. Davenport [Da] independently proved in an elementary manner that

$$V_6(p) \ll p^4,$$

which leads to the result that the exponent in (1) can be reduced from $3/4$ to $2/3$ up to the constant factor. On the other hand, it follows from the work in [HSvv] that

$$V_6(p) = 5p^4 - 10p^3 - (b_p + 9)p^2 - 5p - 1, \quad p > 7,$$

where b_p is the integer with $|b_p| < 2p^{3/2}$ defined to be the p -th Fourier coefficient in the Fourier expansion of the newform of weight 4, level 6 given by $(\eta(z)\eta(2z)\eta(3z)\eta(6z))^2$, here η is the Dedekind eta function.

In a recent paper, R. J. Evans [Ev] studied the case of $k = 7$ and conjecturely obtained an exact identity in terms of Hecke eigenvalues for a weight 3 newform on $\Gamma_0(525)$ with quartic nebentypus of conductor 105.

However, for the cases $k \geq 8$, it seems that there are not too many works focusing on the identities of moments of Kloosterman sums. It should be remarked that N. M. Katz [Ka] has studied the higher moments from a modern point of view. From his result, one can deduce certain asymptotic formulae for any even power moments of $S(a, 1; p)$. However, we can just obtain upper bounds for the case of odd powers, and it seems that to get an asymptotic formula valid for a general odd integer k is out of reach at present.

Theorem 1. *For any given natural number k and each large prime number p , we have*

$$V_{2k}(p) = \frac{1}{k+1} \binom{2k}{k} p^{k+1} + O(p^{k+1/2}),$$

$$V_{2k+1}(p) \ll p^{k+1},$$

where $\binom{m}{n}$ is the binomial coefficient defined as $m!/n!(m-n)!$, and the implied constants depend only on k .

In fact, if we apply Weil's bound (2) to each individual Kloosterman sum and then summing over a , we can deduce the rough estimate

$$|V_{2k+1}(p)| \leq \sum_{a \bmod p}^* |S(a, 1; p)|^{2k+1} \ll p^{k+3/2}.$$

Hence one can expect that there must be significant cancellations among these individual Kloosterman sums in $V_{2k+1}(p)$. In order to illustrate this phenomenon, we would like to investigate the following moments of *absolute* Kloosterman sums:

$$\tilde{V}_k(p) = \sum_{a \bmod p}^* |S(a, 1; p)|^k.$$

In fact, we can establish an asymptotic formula for $\tilde{V}_k(p)$ as p tends to infinity.

Theorem 2. *For any given natural number k and each large prime number p , we have*

$$\tilde{V}_{2k+1}(p) = \frac{4^{k+1}}{\pi(2k+1)(2k+3)} \binom{2k}{k}^{-1} p^{k+3/2} + O_k(p^{k+1}),$$

where the implied constant depends only on k .

Subsequently, we can deduce from Theorems 1 and 2 that

Corollary. *For sufficiently large prime number p , we have*

$$\sum_{\substack{a \bmod p \\ S(a,1;p) > 0}}^* 1 \geq \frac{4}{9\pi^2} p + O(p^{1/2}),$$

and

$$\sum_{\substack{a \bmod p \\ S(a,1;p) < 0}}^* 1 \geq \frac{4}{9\pi^2} p + O(p^{1/2}).$$

We shall give the proof of the theorems along the line of the following sections. First, we shall review some basic properties of Chebyshev polynomials in Section 2, and then we shall deduce the theorems from Katz's result on Kloosterman sheaves, which will be completed in Section 3. The proof of the corollary will be completed in Section 4.

2. CHEBYSHEV POLYNOMIALS

The Chebyshev polynomials $U_k(x)$ ($k \geq 0$) are defined recursively by

$$U_0(x) = 1, \quad U_1(x) = 2x,$$

$$U_{k+1}(x) = 2xU_k(x) - U_{k-1}(x).$$

Chebyshev polynomials enjoy the following identity

$$\frac{2}{\pi} \int_{-1}^1 \sqrt{1-x^2} U_m(x) U_n(x) dx = \begin{cases} 1, & m = n, \\ 0, & m \neq n. \end{cases}$$

This shows that Chebyshev polynomials are orthogonal with respect to the weight

$$\frac{2}{\pi} \sqrt{1-x^2}$$

on the interval $[-1, 1]$. Hence one may expect that every continuous function defined in $[-1, 1]$ can be represented by a certain linear combination of such Chebyshev polynomials. In particular, we have

Lemma 1 ([Ri], P.54). *For each $k \in \mathbb{N}$ and $x \in [-1, 1]$, we have*

$$(3) \quad x^{2k} = \frac{(2k)!}{4^k} \sum_{0 \leq \ell \leq k} \frac{2\ell + 1}{(k-\ell)!(k+\ell+1)!} U_{2\ell}(x),$$

and

$$(4) \quad x^{2k+1} = \frac{(2k+1)!}{4^{k+1}} \sum_{0 \leq \ell \leq k} \frac{\ell + 1}{(k-\ell)!(k+\ell+2)!} U_{2\ell+1}(x).$$

Moreover, we can express $|x|^{2k+1}$ as a linear combination of certain Chebyshev polynomials as follows:

$$|x|^{2k+1} = \sum_{\ell \geq 0} a_\ell U_\ell(x),$$

where the coefficients a_j 's could be computed in the following manner:

$$a_\ell = \frac{2}{\pi} \int_{-1}^1 \sqrt{1-x^2} U_\ell(x) |x|^{2k+1} dx.$$

First we have

$$a_\ell = \frac{2}{\pi} \int_0^1 \sqrt{1-x^2} x^{2k+1} (U_\ell(x) + U_\ell(-x)) dx.$$

Putting $x = \cos \theta$, we obtain that

$$\begin{aligned} a_\ell &= \frac{2}{\pi} \int_{\pi/2}^0 \sin \theta (\cos \theta)^{2k+1} (U_\ell(\cos \theta) + U_\ell(-\cos \theta)) d \cos \theta \\ &= \frac{2}{\pi} \int_0^{\pi/2} \sin^2 \theta (\cos \theta)^{2k+1} (U_\ell(\cos \theta) + U_\ell(-\cos \theta)) d\theta. \end{aligned}$$

Since

$$U_\ell(\cos \theta) = \frac{\sin((\ell+1)\theta)}{\sin \theta}, \quad U_\ell(-\cos \theta) = (-1)^\ell \frac{\sin((\ell+1)\theta)}{\sin \theta},$$

it follows that

$$a_\ell = \frac{2}{\pi} (1 + (-1)^\ell) \int_0^{\pi/2} \sin \theta (\cos \theta)^{2k+1} \sin((\ell+1)\theta) d\theta.$$

Thus $a_\ell = 0$ if ℓ is odd, and if ℓ is even, we have

$$(5) \quad a_\ell = \frac{4}{\pi} \int_0^{\pi/2} \sin \theta (\cos \theta)^{2k+1} \sin((\ell+1)\theta) d\theta.$$

For $\ell = 0$, we have

$$a_0 = \frac{4}{\pi} \int_0^{\pi/2} \sin^2 \theta (\cos \theta)^{2k+1} d\theta = \frac{4^{k+1}}{\pi(2k+1)(2k+3)} \binom{2k}{k}^{-1}.$$

For $\ell \geq 2k+2$, we have

$$a_\ell = \frac{2}{\pi} \int_0^{\pi/2} (\cos(\ell\theta) - \cos((\ell+2)\theta)) (\cos \theta)^{2k+1} d\theta,$$

then it follows that (by [RG], 2.538)

$$a_\ell = \frac{2}{\pi} \left(\frac{(-1)^{\ell/2+k+1} (2k+1)!}{(2k+1+\ell)(\ell-2k-1)!} - \frac{(-1)^{\ell/2+k} (2k+1)!}{(2k+3+\ell)(\ell-2k+1)!} \right).$$

Moreover, we have

$$a_\ell \ll \frac{1}{(\ell-2k)!}$$

for any $\ell \geq 2k+2$, where the implied constant depends only on k .

Hence we can conclude that

Lemma 2. *For each $k \in \mathbb{N}$ and $x \in [-1, 1]$, we have*

$$(6) \quad |x|^{2k+1} = \frac{4^{k+1}}{\pi(2k+1)(2k+3)} \binom{2k}{k}^{-1} + \sum_{\ell \geq 1} c_{\ell,k} U_{2\ell}(x),$$

where $c_{\ell,k} = a_{2\ell}$ could be computed exactly by (5) for $1 \leq \ell \leq k$ and is bounded as

$$c_{\ell,k} \ll_k \frac{1}{(2\ell - 2k)!}$$

for $\ell \geq k + 1$.

3. DERIVATION FROM KATZ'S ESTIMATE

In view of Weil's bound (2), we can write

$$(7) \quad \frac{S(a, 1; p)}{\sqrt{p}} = 2 \cos \theta_p(a),$$

where $0 \leq \theta_p(a) \leq \pi$ is called the Kloosterman sum angle.

The main result of N. M. Katz [Ka] can be stated equivalently as follows.

Proposition (see [Iw], Theorem 4.6). *For any positive integer k and odd prime p , we have*

$$(8) \quad \left| \sum_{a \bmod p}^* U_k(\cos \theta_p(a)) \right| \leq \frac{1}{2}(k+1)p^{1/2}.$$

Following the notation in (7), we have

$$V_{2k}(p) = (4p)^k \sum_{a \bmod p}^* (\cos \theta_p(a))^{2k},$$

from which and (3), we can deduce that

$$V_{2k}(p) = p^k (2k)! \sum_{0 \leq \ell \leq k} \frac{2\ell + 1}{(k - \ell)!(k + \ell + 1)!} \sum_{a \bmod p}^* U_{2\ell}(\cos \theta_p(a)).$$

The term $\ell = 0$ gives the contribution

$$(9) \quad p^k \frac{(2k)!}{k!(k+1)!} \sum_{a \bmod p}^* U_0(\cos \theta_p(a)) = \frac{1}{k+1} \binom{2k}{k} p^{k+1} + O(p^k),$$

where the O -constant depends only on k . For the terms with $1 \leq \ell \leq k$, we can apply Katz's estimate (8) to each one, getting

$$(10) \quad p^k (2k)! \sum_{1 \leq \ell \leq k} \frac{2\ell + 1}{(k - \ell)!(k + \ell + 1)!} \sum_{a \bmod p}^* U_{2\ell}(\cos \theta_p(a)) \ll_k p^{k+1/2}.$$

Combining (9) and (10), we finally arrive at

$$V_{2k}(p) = \frac{1}{k+1} \binom{2k}{k} p^{k+1} + O(p^{k+1/2}),$$

where the O -constant depends only on k .

Following a similar argument, we can write

$$V_{2k+1}(p) = \frac{1}{2} (2k+1)! p^{k+1/2} \sum_{0 \leq \ell \leq k} \frac{\ell + 1}{(k - \ell)!(k + \ell + 2)!} \sum_{a \bmod p}^* U_{2\ell+1}(\cos \theta_p(a)).$$

Applying Katz's estimate (8), we can find that

$$V_{2k+1}(p) \ll p^{k+1}.$$

This completes the proof of Theorem 1. And Theorem 2 follows in a similar way, since for any fixed k , the coefficient $c_{\ell,k}$ in Lemma 2 decays rapidly as ℓ tends to infinity.

4. PROOF OF THE COROLLARY

Observing that

$$\sum_{\substack{a \bmod p \\ S(a,1;p) > 0}}^* S(a,1;p) = \frac{1}{2}(V_1(p) + \tilde{V}_1(p)),$$

thus we can conclude from Theorems 1 and 2 that

$$(11) \quad \sum_{\substack{a \bmod p \\ S(a,1;p) > 0}}^* S(a,1;p) = \frac{1}{3\pi} p^{3/2} + O(p).$$

On the other hand, from Cauchy inequality we have

$$\left(\sum_{\substack{a \bmod p \\ S(a,1;p) > 0}}^* S(a,1;p) \right)^2 \leq V_2(p) \sum_{\substack{a \bmod p \\ S(a,1;p) > 0}}^* 1,$$

it follows from (11) and Theorem 1 that

$$\sum_{\substack{a \bmod p \\ S(a,1;p) > 0}}^* 1 \geq \frac{1}{V_2(p)} \left(\sum_{\substack{a \bmod p \\ S(a,1;p) > 0}}^* S(a,1;p) \right)^2 = \frac{4}{9\pi^2} p + O(p^{1/2}).$$

Similarly, we also have

$$\sum_{\substack{a \bmod p \\ S(a,1;p) < 0}}^* 1 \geq \frac{4}{9\pi^2} p + O(p^{1/2}).$$

5. ADDITIONAL REMARKS

In a recent paper, D. I. Tolev [To] obtained by elementary methods a smart identity of $S(a, b; p)$ for an arbitrary odd prime p and $(ab, p) = 1$. Namely,

$$S^2(a, b; p) = p + \sum_{x \bmod p} \left(\frac{x^2 - 4x}{p} \right) S(a, bx, p).$$

From this identity, he can easily deduce that

$$|S(a, b; p)| \leq \sqrt{p + p^{3/2}}, \quad (ab, p) = 1,$$

which is of a smaller constant factor than the previous result of H. D. Kloosterman.

Of course, one may expect there exist certain identities for higher moments (especially for odd power moments) of Kloosterman sums. This still remains blank, however it seems a meaningful direction.

On the other hand, many arithmetical problems lead us to deal with the general Kloosterman sum twisted by a Dirichlet character $\chi \pmod{p}$, which is defined by

$$S_\chi(a, b; p) = \sum_{x \bmod p}^* \chi(x) e\left(\frac{ax + b\bar{x}}{p}\right).$$

If χ is the principal character, this reduces to classical Kloosterman sum $S(a, b; p)$, if χ is the Legendre symbol mod p , this is known as the Salié sum. Following Tolev's idea, one can find the following identity

$$|S_\chi(a, b; p)|^2 = p - 1 + \sum_{x \bmod p}^* S_\chi(x, x; p) e\left(-\frac{2x + ab\bar{x}}{p}\right)$$

holds for any $\chi \bmod p$ and $(ab, p) = 1$. Notice that $S_\chi^2(a, b; p) = \chi(-\overline{ab})|S_\chi(a, b; p)|^2$, $(ab, p) = 1$, thus a corresponding identity also holds for $S_\chi^2(a, b; p)$. Moreover, one can also deduce the following upper bounds that for $(ab, p) = 1$,

$$|S_\chi(a, b; p)| < \begin{cases} 2^{1/4}p^{3/4}, & \text{if } \chi = \left(\frac{\cdot}{p}\right), \\ p^{3/4}, & \text{if } \chi \neq \left(\frac{\cdot}{p}\right). \end{cases}$$

In closing, we would like to mention a twisted moment of Kloosterman sums studied by C. L. Liu [L]. He proved that

$$\sum_{a \bmod p}^* \chi(a) U_k(\cos \theta_p(a)) \ll_k p^{1/2}$$

holds for any positive integer k and odd prime p , where χ is a non-real character mod p . Clearly, his estimate yields

$$\sum_{a \bmod p}^* \chi(a) S^{2k}(a, 1; p) \ll_k p^{k+1/2},$$

which shows that there must be significant cancellations because of the existence of the character χ . Regarding the case of odd powers, it follows that

$$\sum_{a \bmod p}^* \chi(a) S^{2k+1}(a, 1; p) \ll_k p^{k+1}$$

and

$$\sum_{a \bmod p}^* \chi(a) |S^{2k+1}(a, 1; p)| \ll_k p^{k+1}.$$

Acknowledgements. The present paper was prepared as YY participated in the 5th National Conference in Number Theory held in Zhaoqing. Both authors are grateful to Prof. C. L. Liu for his helpful suggestions during the conference, and to the referee for the valuable advice and comments. The work of the authors is supported by the Fundamental Research Funds for the Central Universities.

REFERENCES

- [Da] H. Davenport, On certain exponential sums, *J. Reine Angew. Math.*, **169** (1933), 158-176.
- [Ev] R. J. Evans, Seventh power moments of Kloosterman sums, *Israel J. Math.*, **175** (2010), 349-362.
- [HSvv] K. Hulek, J. Spandaw, B. van Geemen & D. van Straten, The modularity of the Barth-Nieto quintic and its relatives, *Adv. Geom.*, **1** (2001), 263-289.
- [Iw] H. Iwaniec, Topics in classical automorphic forms, AMS Graduate Studies in Math **17**, Amer. Math. Soc., 1997.
- [Ka] N. M. Katz, Sommes exponentielles (in French), *Asterisque*, **79** (1980).
- [Kl] H. D. Kloosterman, On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$, *Acta Math.*, **49** (1926), 407-464.
- [L] C. L. Liu, Twisted higher moments of Kloosterman sums, *Proc. Amer. Math. Soc.*, **130** (2002), 1887-1892.
- [Li] R. Livné, Motivic orthogonal two-dimensional representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Israel J. Math.*, **92** (1995), 149-156.
- [PTV] C. Peters, J. Top & M. van der Vlugt, The Hasse zeta function of a $K3$ surface related to the number of words of weight 5 in the Melas codes, *J. Reine Angew. Math.*, **432** (1992), 151-176.
- [Po] H. Poincaré, Fonctions modulaires et fonctions fuchsienues, *Ann. Fac. Sci. Toulouse*, **3** (1911), 125-149.
- [Ri] J. Riordan, Combinatorial Identities, John Wiley, New York, 1968.
- [RG] I. M. Ryzhik & I. S. Gradshteyn, Tables of Integrals, Series and Products (Seventh Edition), Elsevier, 2007.
- [Sa] H. Salié, Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen. *Math. Z.*, **36** (1933), 263-278.

- [Sch] W. Schmidt, Equations over Finite Fields: An Elementary Approach, Lecture Notes in Math., **536**, Springer, Berlin, 1976.
- [To] D. I. Tolev, An identity for the Kloosterman sum, <http://arxiv.org/abs/1007.2054>.
- [We] A. Weil, On some exponential sums, *Proc. Nat. Acad. Sci. U.S.A.*, **34** (1948), 204-207.

SCHOOL OF SCIENCE, XI'AN JIAOTONG UNIVERSITY, XI'AN 710049, P. R. CHINA
E-mail address: `xprime@163.com`